In the Claims:

1. [Original] A method for a sender to send an encrypted message to an authorized recipient, the method having steps comprising:

creating an encrypted content message that may be decrypted using a content decryption key that is unknown to the authorized recipient;

creating an encrypted authentication message that may be decrypted using a recipient's key wherein the recipient's key is known to the authorized recipient but unknown to others except perhaps known to the sender;

fixing the encrypted authentication message and the encrypted content message onto a tangible medium and thereafter permitting the authorized recipient to obtain the tangible medium;

if a valid reply has been received, wherein the valid reply is based upon the decrypted authentication message, then allowing the authorized recipient to obtain said content decryption key.

2. [Original] The method of claim 1 wherein the recipient's key is a secret key that is shared between the sender and the recipient.

3. [Original] The method of claim 1 wherein the recipient's key is a recipient's private key that is associated with a recipient's public key.

4. [Original] The method of claim 1 wherein said step of creating an encrypted authentication message further comprises a step of sender authentication encryption such that the authorized recipient may use a sender's key for decryption of the authentication message thereby authenticating that the sender was the source of the encrypted authentication message, such that the sender's key is known to the authorized recipient, and such that the encrypted authentication message may be decrypted with a decryption step employing said recipient's key and with another decryption step employing said sender's key.

5. [Original] The method of claim 4 wherein the sender's key is a secret key that is shared between the sender and the authorized recipient but unknown to others.

6. [Original] The method of claim 4 wherein the sender's key is a public key that is associated with a sender's private key.

7. [Original] The method of claim 1 wherein said step of creating an encrypted content message further comprises a step of sender authentication encryption such that the authorized recipient may use a sender's key for decryption of the encrypted content message thereby authenticating that the sender was the source of the encrypted content message, such that the sender's key is known by the authorized recipient, and such that the encrypted content message may be decrypted by a decryption method with a step employing the recipient's key and with another step employing the sender's key.

8. [Original] The method of claim 7 wherein the sender's key is a secret key that is shared between the sender and the authorized recipient but unknown to others.

9. [Original] The method of claim 4 wherein the sender's key is a public key that is associated with a sender's private key.

10. [Original] An article of manufacture for sending an encrypted message from a sender who possesses a content decryption key to a recipient who possesses a recipient's key, the article, comprising:

a tangible medium;

an encrypted content message fixed on said tangible medium, wherein said encrypted content message may be decrypted using the content decryption key;

an encrypted authentication message fixed on said tangible medium, wherein said encrypted authentication message may be decrypted using the recipient's key;

whereby after the article is delivered to the recipient the recipient may use the recipient's key to decrypt said encrypted authentication message into a decrypted authentication message, the recipient may use the decrypted authentication message to send a valid reply to the sender confirming that the recipient received said article and the sender may then allow the recipient to obtain the content decryption key.

11. [Original] The article of claim 10 wherein the recipient's key is a secret key that is shared between the sender and the recipient.

12. [Original] The article of claim 10 wherein the recipient's key is a recipient's private key that is associated with a recipient's public key.

13. [Original] The article of claim 10 wherein said encrypted authentication message is sender authentication encrypted such that said encrypted authentication message may be decrypted by a decryption method having a step employing the recipient's key and having another step employing a sender's key such that the recipient may use the sender's key to authenticate that the sender was the source of said tangible medium.

14. [Original] The article of claim 13 wherein the sender's key is a secret key that is shared between the sender and the authorized recipient but unknown to others.

15. [Original] The article of claim 13 wherein the sender's key is a public key that is associated with a sender's private key.

16. [Original] The article of claim 10 wherein said encrypted content message is sender authentication encrypted such that said encrypted content message may be decrypted by a decryption method having a step employing the recipient's key and having another step employing a sender's key such that the recipient may use the sender's key to authenticate that the sender was the source of said tangible medium.

17. [Original] The article of claim 16 wherein the sender's key is a secret key that is shared between the sender and the authorized recipient but unknown to others.

18. [Original] The article of claim 16 wherein the sender's key is a public key that is associated with a sender's private key.

19. [Original] A method for an authorized recipient to receive an encrypted message from a sender, the method having steps comprising:

receiving a tangible medium from the sender wherein the tangible medium has fixed upon it an encrypted authentication message and an encrypted content message;

using a recipient's key to decrypt the encrypted authentication message into a decrypted authentication message, wherein the recipient's key is known to the authorized recipient but unknown to others except perhaps known to the sender;

creating a valid reply using the decrypted authentication message;

sending the valid reply to the sender;

if the recipient has received a content decryption key from the sender, then using the content decryption key to decrypt the encrypted content message.

20. [Previously Presented] The method of claim 1 further comprising receiving the valid reply using the sender after permitting the authorized recipient to obtain the tangible medium, and wherein the allowing is responsive to the receiving.

21. [Previously Presented] The method of claim 20 wherein the valid reply is generated by the recipient after the recipient obtains the tangible medium.

22. [Previously Presented] The method of claim 1 wherein the creatings, the fixing and the allowing comprise creatings, fixing and allowing using the sender.

23. [Previously Presented] The method of claim 1 wherein the fixing comprises permanently fixing the encrypted authentication message and the encrypted content message onto said tangible medium.

24. [Previously Presented] The article of claim 10 wherein the encrypted content message and the encrypted authentication message are permanently fixed onto said tangible medium.

25. [Previously Presented] The method of claim 19 wherein the creating and the sending the valid reply comprise creating and sending using the authorized recipient.

26. [Previously Presented] The method of claim 19 wherein the receiving, the usings, the creating, and the sending comprise receiving, usings, creating and sending using the authorized recipient.

27. [New] The method of claim 1 wherein the fixing comprises fixing both the encrypted authentication message and the encrypted content message onto the tangible medium comprising the same medium.

28. [New] The method of claim 27 wherein the same medium comprises a single fixed tangible medium.

29. [New] The method of claim 28 wherein the single fixed tangible medium comprises a compact disc.

30. [New] The method of claim 19 wherein the using the recipient's key comprises using the recipient's key by the authorized recipient.

31. [New] The method of claim 19 wherein the creating the valid reply comprises creating using the authorized recipient.